News Release

United States Navy

Space and Naval Warfare Systems Command
Public Affairs and Corporate Communications
4301 Pacific Highway, San Diego CA 92110-3127
Telephone: 619-524-3432 FAX: 619-524-3469

Release Nr. NR-2001-013
Tuesday, March 13, 2001

SPAWAR Information Security Group Scores a First

NEW ORLEANS — To go where no man has gone before - or in the case of the latest ITC Success Story – to do what no information security group had done before:

> Build a bridge between an unclassified environment and a classified environment that would allow information to successfully transit firewalls on both the sending and receiving side, transit the public Internet securely and successfully decrypt at the receiving end in the same condition that it was sent.

Don Gangemi, Information Security Director at the Information Technology Center and his group successfully pulled off such a feat in response to a need to be able to transmit Defense Integrated Human Resources System (DIMHRS) sensitive unclassified personnel data to the Global Command and Control System (GCCS).

There are three main methods of electronically communicating within the U.S. Government. One is via the Internet which is for non-secure communications generally between government and non-government organizations.

The second method is via the Non-classified Internet Protocol Routing Network or NIPRNET which is the most used method between government, military, and quasi-government organizations.

The third and most secure method is the Secure Internet Protocol Routing Network or SIPRNET. SIPRNET is used for transmitting classified information and is only available to those groups with a specific need to know and have access to classified information.

The challenge that faced the Information Security Group is that security requirements prohibited the direct interconnection between the Internet and NIPRNET or between either of them and the SIPRNET.

To accomplish transmitting data between DIMHRS and the classified GCCS system they built a bridge using a methodology called a "Trusted Guard" technology.

Arrangements were made with the Defense Information Systems Agency (DISA) to acquire and install a Trusted Guard at their Slidell, Louisiana facility and for them to interface that into the SIPRNET.

The next challenge was to find a secure way to transmit the Sensitive Unclassified information in a secure manner to the input side of the Trusted Guard. This was accomplished using a methodology called Internet Protocol Security (IPSec) and a technology within IPSec called Virtual Private Networking (VPN) using a feature called Tunneling.

First the clear text data needing to be transferred was encrypted so that it bore no resemblance to the original data. Even the address where the data was to be sent was encrypted. Then a new address was appended onto the encrypted package which was the address of the encryption device on the other end - in this case the DISA at Slidell.

This encrypted package was then sent over the NIPRNET to the encryption device at the other end. When received, the IP address was stripped away and the remaining package decrypted before being forwarded to the actual recipient where it was fed into the Trusted Guard for further preparation before being sent to the SIPRNET.

The IPSec portion was the encryption of the data. The Tunneling portion was the actual IP address of the recipient that was also encrypted and the IP address of the encryption device substituted. It was referred to as Tunneling because anyone intercepting the message would not be able to tell who the intended recipient was, only that it was going to a device that had no identity attached to it.

Furthermore anyone intercepting the package would be unable to read it because it was encrypted.

There were a number of ways that the IPSec methodology could have been designed which would have been easier to achieve but it would have been less secure. In fact, the methodology used was not one that has been documented previously by anyone but was designed by the ITC Development Information Security Group. The VPN Project Team Leader, Linda Goodwin, has named this design topology the "Secure Parallel Topology." Although this topology was very complex and had no previous installation documentation, it was felt that the high level of security it provided was worth the extra effort in setting it up.

In February, test packages of 10 Megabit (Mb), 100 Mb, 250 Mb, and 500 Mb were successfully sent to the DISA via the VPN set up between DISA and DIMHRS. This success prompted John Erb of the Joint Staff to offer his congratulations to the professionals from within the ITC/DIMHRS Information Security Group, DISA Slidell, and the GCSS whose hard work had made it happen.

Six employees of the Information Technology Center participated in the demonstration project: Linda Goodwin, Lambert LeBleu, Scott Higgins, Gary Wallace, Brian Desormeaux, and Paul Sorensen.

For more information contact:

Maria LoVasco Tolleson, Public Affairs Officer, SPAWAR Information Technology Center New Orleans, 504-697-2073 or e-mail lovascom@cnrf.nola.navy.mil